This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-120. (Canceled)

121. (Currently Amended) A computer-readable medium having stored thereon computer-executable instructions, wherein the instructions, when executed, perform a method to distribute a digital content package from a content server to a computing device within a digital rights management system, the distribution method comprising:

receiving, at the content server, a request to distribute the digital content package; and

distributing the digital content package in response to receiving the request for the digital content package, the digital content package comprising:

~~a data file corresponding to a digital content package, the data structure including:~~

a first data field containing encrypted digital content to be rendered in accordance with a corresponding digital license, the encrypted digital content being decrypt-able according to a decryption key (KD) obtained from the license;

a second data field containing a content ID or a package ID identifying one of the digital content and the digital content package respectively, the corresponding license also having the content ID or the digital content package ID such that the content ID or the digital content package ID from the digital content package is employed to locate the corresponding license; and

a third data field containing license acquisition information including a location of a license provider for providing the license after identifying the digital content ID

or the digital content package ID to such license provider, wherein the license acquisition information is in an unencrypted form;

wherein the license provider location is a network address; and

wherein the ~~data file~~ digital content package is provided to the content server by a content provider having a public key and a private key, the ~~data file~~ digital content package further including a fourth data field containing the content provider public key, the corresponding license including a content provider digital certificate issued and signed by the content provider private key to show permission from the content provider to the license provider to provide the corresponding license, such that the content provider public key from the digital content package is employed to validate the content provider digital certificate of the corresponding license.

122-123. (Canceled)

124. (Previously Presented) The medium of claim 121 wherein the license provider location is an Internet address.

125. (Canceled)

126. (Previously Presented) The medium of claim 121 wherein the content provider public key is encrypted according to the decryption key (KD).

127. (Currently Amended) The medium of claim 126 wherein the encrypted content provider public key is signed by the content provider private key, and wherein alteration of the encrypted content provider public key prevents validation of the digital content package. ~~data file.~~

128. (Currently Amended) The medium of claim 121 wherein the content provider public key is signed by the content provider private key, wherein alteration of the content provider public key prevents validation of the digital content package. ~~data file.~~

129. (Previously Presented) The medium of claim 121 further comprising a fifth data field containing a key ID identifying the decryption key (KD).

130. (Currently Amended) The medium of claim 121 wherein the digital content package ~~data file~~ is provided by a content provider authorized by a root source to provide the digital content package, ~~data file, the data file~~ digital content package further comprising a fifth data field containing a certificate from the root source indicating that the content provider has authority from the root source to provide the digital content package. ~~data file.~~

131. (Previously Presented) The medium of claim 130 wherein the content provider has a public key and a private key, and wherein the certificate includes the public key of the content provider.

132. (Previously Presented) The medium of claim 131 wherein the root source has a public key and a private key, wherein the certificate is signed with the private key of the root source, and wherein the public key of the root source must be obtained to decrypt the encrypted signature.

133. (Currently Amended) The medium of claim 121 wherein the digital content package ~~data file~~ is provided by a content provider authorized by an intermediary source to provide the digital content package, ~~data file,~~ the intermediary source in turn being authorized by a root source to authorize the content provider, the digital content package ~~data file~~ further comprising a fifth data field containing a first certificate from the root source indicating that the intermediary source has authority from the root source to authorize the content provider, and a sixth data field containing a second certificate from the intermediary source indicating that the content provider has authority from the intermediary source to provide the digital content package. ~~data file.~~

134. (Previously Presented) The medium of claim 133 wherein the content provider has a public key and a private key, wherein the intermediary source has a public key and a private key, wherein the first certificate includes the public key of the intermediary source, and wherein the second certificate includes the public key of the content provider.

135. (Previously Presented) The medium of claim 134 wherein the root source has a public key and a private key, wherein the first certificate is signed with the

private key of the root source, wherein the second certificate is signed with the private key of the intermediary source, wherein the public key of the root source must be obtained to decrypt the encrypted signature of the first certificate, and wherein the public key of the intermediary source is obtained from the first certificate to decrypt the encrypted signature of the second certificate.